Appendix 6

(Ref: Para. 25(c)(ii), A173–A174)

Considerations for Understanding General IT Controls

This appendix provides further matters that the auditor may consider in understanding general IT controls.

1. The nature of the general IT controls typically implemented for each of the aspects of the IT environment:

   (a) Applications

   General IT controls at the IT application layer will correlate to the nature and extent of application functionality and the access paths allowed in the technology. For example, more controls will be relevant for highly-integrated IT applications with complex security options than a legacy IT application supporting a small number of account balances with access methods only through transactions.

   (b) Database

   General IT controls at the database layer typically address risks arising from the use of IT related to unauthorised updates to financial reporting information in the database through direct database access or execution of a script or program.

   (c) Operating system

   General IT controls at the operating system layer typically address risks arising from the use of IT related to administrative access, which can facilitate the override of other controls. This includes actions such as compromising other user's credentials, adding new, unauthorised users, loading malware or executing scripts or other unauthorised programs.

   (d) Network

   General IT controls at the network layer typically address risks arising from the use of IT related to network segmentation, remote access, and authentication. Network controls may be relevant when an entity has web-facing applications used in financial reporting. Network controls are also may be relevant when the entity has significant business partner relationships or third-party outsourcing, which may increase data transmissions and the need for remote access.

2. Examples of general IT controls that may exist, organised by IT process include:

   (a) Process to manage access:

   - *Authentication*

     Controls that ensure a user accessing the IT application or other aspect of the IT environment is using the user's own log-in credentials (i.e., the user is not using another user's credentials).

   - *Authorisation*

     Controls that allow users to access the information necessary for their job responsibilities and nothing further, which facilitates appropriate segregation of duties.

- *Provisioning*

  Controls to authorise new users and modifications to existing users' access privileges.

- *Deprovisioning*

  Controls to remove user access upon termination or transfer.

- *Privileged access*

  Controls over administrative or powerful users' access.

- *User access reviews*

  Controls to recertify or evaluate user access for ongoing authorisation over time.

- *Security configuration controls*

  Each technology generally has key configuration settings that help restrict access to the environment.

- *Physical access*

  Controls over physical access to the data centre and hardware, as such access may be used to override other controls.

(b) Process to manage program or other changes to the IT environment:

- *Change management process*

  Controls over the process to design, program, test and migrate changes to a production (i.e., end user) environment.

- *Segregation of duties over change migration*

  Controls that segregate access to make and migrate changes to a production environment.

- *Systems development or acquisition or implementation*

  Controls over initial IT application development or implementation (or in relation to other aspects of the IT environment).

- *Data conversion*

  Controls over the conversion of data during development, implementation or upgrades to the IT environment.

(c) Process to manage IT operations

- *Job scheduling*

  Controls over access to schedule and initiate jobs or programs that may affect financial reporting.

- *Job monitoring*

Controls to monitor financial reporting jobs or programs for successful execution.

- *Backup and recovery*

  Controls to ensure backups of financial reporting data occur as planned and that such data is available and able to be accessed for timely recovery in the event of an outage or attack.

- *Intrusion detection*

  Controls to monitor for vulnerabilities and or intrusions in the IT environment.

The table below illustrates examples of general IT controls to address examples of risks arising from the use of IT, including for different IT applications based on their nature.

Process	Risks	Controls	IT Applications		
IT Process	Example Risks Arising from the Use of IT	Example General IT Controls	Non-complex commercial software – Applicable (yes / no)	Mid-size and moderately complex commercial software or IT applications – Applicable (yes / no)	Large or complex IT applications (e.g., ERP systems) – Applicable (yes / no)
Manage Access	User-access privileges: Users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.	Management approves the nature and extent of user-access privileges for new and modified user access, including standard application profiles/roles, critical financial reporting transactions, and segregation of duties	Yes – instead of user access reviews noted below	Yes	Yes
		Access for terminated or transferred users is removed or modified in a timely manner	Yes – instead of user access reviews below	Yes	Yes

		User access is periodically reviewed	Yes – instead of provisioning / Deprovisioning controls above	Yes – for certain applications	Yes
		Segregation of duties is monitored and conflicting access is either removed or mapped to mitigating controls, which are documented and tested	N/A – no system enabled segregation	Yes – for certain applications	Yes
		Privileged-level access (e.g., configuration, data and security administrators) is authorised and appropriately restricted	Yes – likely at IT application layer only	Yes – at IT application and certain layers of IT environment for platform	Yes – at all layers of IT environment for platform
Manage Access	Direct data access: Inappropriate changes are made directly to financial data through means other than application transactions.	Access to application data files or database objects/tables/data is limited to authorised personnel, based on their job responsibilities and assigned role, and such access is approved by management	N/A	Yes – for certain applications and databases	Yes
Manage Access	System settings: Systems are not adequately configured or updated to restrict system access to properly	Access is authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users are	Yes – password authentication only	Yes – mix of password and multi-factor authentication	Yes

	authorised and appropriate users.	authorised to gain access to the system. Password parameters meet company or industry standards (e.g., password minimum length and complexity, expiration, account lockout)			
		The key attributes of the security configuration are appropriately implemented	N/A – no technical security configuratio ns exist	Yes – for certain applications and databases	Yes
Manage Change	Application changes: Inappropriate changes are made to application systems or programs that contain relevant automated controls (i.e., configurable settings, automated algorithms, automated calculations, and automated data extraction) or report logic.	Application changes are appropriately tested and approved before being moved into the production environment	N/A – would verify no source code installed	Yes – for non-commercial software	Yes
		Access to implement changes into the application production environment is appropriately restricted and segregated from the development environment	N/A	Yes for non-commercial software	Yes
Manage Change	Database changes: Inappropriate changes are made to the database structure and relationships between the data.	Database changes are appropriately tested and approved before being moved into the	N/A – no database changes made at entity	Yes – for non-commercial software	Yes

		production environment			
Manage Change	System software changes: Inappropriate changes are made to system software (e.g., operating system, network, change-management software, access-control software).	System software changes are appropriately tested and approved before being moved to production	N/A – no system software changes are made at entity	Yes	Yes
Manage Change	Data conversion: Data converted from legacy systems or previous versions introduces data errors if the conversion transfers incomplete, redundant, obsolete, or inaccurate data.	Management approves the results of the conversion of data (e.g., balancing and reconciliation activities) from the old application system or data structure to the new application system or data structure and monitors that the conversion is performed in accordance with established conversion policies and procedures	N/A – Addressed through manual controls	Yes	Yes
IT Operations	Network: The network does not adequately prevent unauthorised users from gaining inappropriate access to information systems.	Access is authenticated through unique user IDs and passwords or other methods as a mechanism for validating that users are authorised to gain access to the system. Password parameters meet company or professional policies and	N/A – no separate network authenticati on method exists	Yes	Yes

		standards (e.g., password minimum length and complexity, expiration, account lockout)			
		Network is architected to segment web-facing applications from the internal network, where ICFR relevant applications are accessed	N/A – no network segmentation employed	Yes – with judgement	Yes – with judgement
		On a periodic basis, vulnerability scans of the network perimeter are performed by the network management team, which also investigates potential vulnerabilities	N/A	Yes – with judgement	Yes – with judgement
		On a periodic basis, alerts are generated to provide notification of threats identified by the intrusion detection systems. These threats are investigated by the network management team	N/A	Yes – with judgement	Yes – with judgement
		Controls are implemented to restrict Virtual Private Network (VPN) access to	N/A – no VPN	Yes – with judgement	Yes – with judgement

		authorised and appropriate users			
IT Operations	Data backup and recovery: Financial data cannot be recovered or accessed in a timely manner when there is a loss of data.	Financial data is backed up on a regular basis according to an established schedule and frequency	N/A – relying on manual backups by finance team	Yes	Yes
IT Operations	Job scheduling: Production systems, programs, or jobs result in inaccurate, incomplete, or unauthorised processing of data.	Only authorised users have access to update the batch jobs (including interface jobs) in the job scheduling software	N/A – no batch jobs	Yes – for certain applications	Yes
		Critical systems, programs, or jobs are monitored, and processing errors are corrected to ensure successful completion.	N/A – no job monitoring	Yes – for certain applications	Yes